UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,801	01/22/2002	Uma Chandrashekhar	CHANDRASHEKHAR 1-2-1-2-2-	4733

46363 7590 02/01/2010

WALL & TONG, LLP/
ALCATEL-LUCENT USA INC.
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
DOAN, DUYEN MY	
ART UNIT	**PAPER NUMBER**
2452	

MAIL DATE	DELIVERY MODE
02/01/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte UMA CHANDRASHEKHAR, MOHAMED L. EL-SAYED,
KENNETH J. JOHNSON, ANDREW R. MCGEE, STEVEN H RICHMAN,
and S. RAO VASIREDDY

Appeal 2009-005560
Application 10/053,801[1]
Technology Center 2400

Decided: February 1, 2010

Before KENNETH W. HAIRSTON, MARC S. HOFF,
and KARL D. EASTHOM, *Administrative Patent Judges.*

HOFF, *Administrative Patent Judge.*

DECISION ON APPEAL

[1] The real party in interest is Lucent Technologies, Inc.

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from a Final Rejection of claims 1, 2, and 4-36.[2] We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

Appellants' invention concerns a system and method for dynamically managing IP Virtual Private Networks (VPNs) in a manner enabling subscriber access to IP VPN services on an as-needed basis. The system includes a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network, each of the IP services aggregation switches communicating with at least one respective user through at least one enhanced integrated access device (EIAD). A dynamic virtual private network (VPN) provides customer network management and policy server functions including a user interface enabling remote management of a VPN by a user; wherein the VPN having a defined quality of service (QoS) parameter and a defined security parameter with associated billing rates, at least one of the QoS parameter and the security parameter being adapted in response to user commands provided to the dynamic VPN manager. The dynamic VPN manager adapts at least one of the IP services aggregation switches and at least one of the EIAD to provide a bidirectional QoS for at least one IP flow (Spec. 3:3-16, 8:2-11, 10:27-31).

Claim 1 is exemplary:

1. Apparatus, comprising:

a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network, each of said IP services aggregation switches communicating with at least

[2] Claim 3 has been cancelled.

one respective VPN customer user, wherein said IP services aggregation switches communicate with said at least one VPN customer user via at least one enhanced integrated access device (EIAD); and

a dynamic virtual private network (VPN) manager, for providing customer network management and policy server functions, including a user interface enabling remote management of a VPN by a VPN customer user;

said VPN having at least one of a defined quality of service (QoS) parameter, a defined security parameter and a corresponding billing rate, at least one of said QoS parameter and said security parameter being adapted in response to user commands provided to said dynamic VPN manager by said VPN customer user;

said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS for at least one IP flow.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Forslöw	US 2002/0069278 A1	Jun. 6, 2002
Chanda	US 2002/0095498 A1	Jul. 18, 2002
Pirot	US 6,856,676 B1	Feb. 15, 2005
Duffield	US 6,912,232 B1	Jun. 28, 2005

The Examiner rejected claims 1-17 under 35 U.S.C. § 112, second paragraph, as failing to set forth the subject matter which Applicants regard as their invention.[3]

Claims 1, 2, 4-20, 25-30, and 33-36 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Chanda in view of Pirot and further in view of Duffield.

[3] The Examiner has withdrawn this rejection (Ans. 14).

Claims 21-24, 31, and 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Chanda in view of Pirot and further in view of Duffield and Forslow.

Rather than repeat the arguments of Appellants or the Examiner, we make reference to the Appeal Brief (filed October 15, 2007), the Reply Brief (filed February 5, 2008), and the Examiner's Answer (mailed December 5, 2007) for their respective details.

ISSUE

The Examiner finds that Chanda discloses a service provider that corresponds to the dynamic VPN manger (Ans. 15). The Examiner finds that Chanda discloses that the service provider uses an Integrated Access Device (IAD) and a gateway device to provide clients with numerous service features (Ans. 15). The Examiner finds that the gateway device disclosed in Chanda corresponds to the Internet Protocol (IP) services aggregation switch (Ans. 15). The Examiner finds that the IAD disclosed in Chanda corresponds to the Enhanced Integrated Access Device (EIAD) (Ans. 15). Therefore, the Examiner concludes that Chanda meets the claim limitation of "VPN manager adapting at least one of said IP services aggregation switches and at least one of said ElAD to provide a bidirectional QoS for at least one IP flow" (Ans. 15).

Appellants contend that the combination of Chanda, Pirot, and Duffield fails to teach or suggest the limitation of "said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS (quality of service) for at least one IP flow" as required by claim 1 (App. Br. 14).

Appellants' contentions present us with the following issue:

Did Appellants show that the Examiner erred in finding that the combination of Chanda, Pirot, and Duffield teaches a dynamic VPN manager that adapts at least one of the IP services aggregation switches and at least one of the EIAD to provide a bidirectional QoS (quality of service) for at least one IP flow within a system that dynamically manages an IP Virtual Private Network (VPN)?

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

The Invention

1. According to Appellants, the invention concerns a system and method for dynamically managing IP Virtual Private Networks (VPNs) in a manner enabling subscriber access to IP VPN services on an as-needed basis. The system includes a plurality of internet protocol (IP) services aggregation switches for communicating between respective access networks and a core network, each of the IP services aggregation switches communicating with at least one respective user through at least one enhanced integrated access device (EIAD). A dynamic virtual private network (VPN) manager provides customer network management and policy server functions including a user interface enabling remote management of a VPN by a user; wherein the VPN having a defined quality of service (QoS) parameter and a defined security parameter with associated billing rates, at least one of the QoS parameter and the security parameter being adapted in response to user commands provided to the dynamic VPN manager. The

dynamic VPN manager adapts at least one of the IP services aggregation switches and at least one of the EIAD to provide a bidirectional QoS for at least one IP flow (Spec. 3:3-16, 8:2-11, 10:27-31).

Chanda

2. Chanda teaches a network system 100 that provides clients with fast, flexible, and scalable data communication capability. Using gateway device 102 and IAD 104, a service provider can provide clients with numerous service features. Each client may purchase a different amount of bandwidth according to his or her needs. The clients may be provided with the ability to dynamically increase or decrease the amount of bandwidth purchased in real time. The data being transmitted or received by each client may be prioritized using various parameters to ensure that the higher priority information is generally transmitted before the lower priority information. Clients may be provided with different service plans, where some pay for only the actual amount of the bandwidth used in a particular billing period, where as others may sign onto a monthly plan for a specific amount of bandwidth. Yet other clients may be provided with a combination of the above two plans, where the clients sign on for a specific amount of bandwidth, and pay additional fees for the bandwidth used in excess of the purchased amount (paras. [0029] and [0047]).

3. Chanda discloses a traffic shaper 212 which plays an important role within the gateway device in controlling the data flow. The traffic shaper ensures higher priority packets are given priority over lower priority packets during data transmission (Fig. 6, para. [0051]). The procedure used by the traffic shaper 212 to transmit packets are similar for both the inward-

bound data received from the traffic regulator and the outward-bound data received from the routing device (para. [0055]).

Pirot

4. Pirot teaches a system and method of controlling and managing Internet protocol services in a voice/data telecommunications network having a service assurance and monitoring unit that includes a customer network management unit 170 that provides interfaces to virtual private network (VPN) customers to perform dedicated network management functions. The customer network management unit 170 provides views and reporting of data to the customer as well as provides the VPN customer with the ability to configure certain service parameters (Figs. 2 and 3; col. 1, ll. 14-39; col. 10, ll. 14-39).

5. A VPN operator may run a remote service management subsystem user interface hosted on a small portable computer such as a laptop PC that allows entry into a network operator database. The network operator can control the overall operations of the VPN, and impose some additional limitations. He may also manage and control the service level agreed with the VPN operator on the service management subsystem 52, e.g. by applying VPN access port management (Figs. 2 and 3; col. 11, ll. 42-67).

Duffield

6. Duffield teaches apparatus and methods for a hose VPN system that includes customer networks (202-208) associated with a single hose (210-216) that connects to access points (218-224) of the IP network 250. The hose is a single interface to the VPN for communication to all other endpoints of the VPN. The VPN achieves network resource allocation efficiency by exploiting resource sharing possibilities via multiplexing

routing paths between endpoints and dynamic resource allocation techniques that permit real time resource allocation resizing (Abstract, col. 3, ll. 4-65;).

7. The customer network provides a service level agreement (SLA) for its associated hose. The SLA for each of the hoses may be based on one or more Quality of Service (QoS) requirements. The VPN service provider guarantees that the hose profile is met for each of the hoses. The SLA for hoses may be based on traffic characteristics such as reasonable delay, packet loss rates, jitter, bandwidth minimums, and the like for various time periods. For example, an IP voice VPN service provider might require tight bounds on the per-packet loss rates, delay, and possibly the amount of jitter. The interface between the customer networks 202-208 and the associated hoses 210-216 may be managed by either the customer or the VPN service provider (col. 3, ll. 4-65; col. 4, ll. 10-26,).

8. The customer may manage the outgoing hose traffic by controlling the rate of data packets output through the hoses 210-216 from different applications based on a priority scheme. Thus, higher priority applications may output more data packets than lower priority applications (col. 4, l. 64- col. 5, l. 1).

Forslow

9. Forslow teaches a network-based mobile workgroup system that is an access management system for mobile users with VPN and firewall functionality inbuilt. The mobile user can access the mobile workgroup system over a set of access technologies and select server resources and correspondent nodes to access pending their workgroup membership approvals. All workgroup policy rules are defined in a mobile service manager and pushed down to one or more mobile service routers for

policy enforcement. The mobile service router closest to the mobile client, and being part of the mobile virtual private network, performs regular authentication checks of the mobile client during service execution. At the same time it performs traffic filtering based on the mobile user's workgroup memberships. These two components constitute a security lock, effectively isolating a distributed workgroup into a mobile virtual private network (Abstract, para. [0088]).

10. Forslow discloses the definition for various types of radio access networks in 3G networks, including the Universal Mobile Telecommunications System (UMTS) (paras. [0020-24]).

PRINCIPLES OF LAW

On the issue of obviousness pursuant to 35 U.S.C § 103, the Supreme Court has stated that “the obviousness analysis cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 419 (2007). Further, the Court stated “[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *Id.* at 416. “One of the ways in which a patent’s subject matter can be proved obvious is by noting that there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent’s claims.” *Id.* at 419-420.

The determination of obviousness must consider, *inter alia*, whether a person of ordinary skill in the art would have been motivated to combine the prior art to achieve the claimed invention and whether there would have been a reasonable expectation of success in doing so. *Brown & Williamson*

Tobacco Corp. v. Philip Morris Inc., 229 F.3d 1120, 1125 (Fed. Cir. 2000). Where the teachings of two or more prior art references conflict, the Examiner must weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another. *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991). If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984). Further, our reviewing court has held that "[a] reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994); *Para-Ordnance Mfg., Inc. v. SGS Importers Int'l., Inc.,* 73 F.3d 1085, 1090 (Fed. Cir. 1995).

In determining the scope of the claim, a claim limitation within an 'adapted to,' 'adapted for,' 'wherein' and "whereby' clause that suggests or makes optional but does not require steps to be performed or limit the structure may be ignored. Specifically, "a 'whereby' clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited" *Minton v. Nat'l Ass'n of Securities Dealers, Inc.*, 336 F.3d 1373, 1381 (Fed. Cir. 2003). However, the court held that when a "'whereby' clause states a condition that is material to patentability, it cannot be ignored in order to change the substance of the invention" *Hoffer v. Microsoft Corp.*, 405 F.3d 1326, 1329 (Fed. Cir. 2005).

ANALYSIS

Claims 1, 2, 4-20, 25-30 and 33-36

The Examiner finds that Chanda discloses a service provider that corresponds to the dynamic VPN manger (Ans. 15). The Examiner finds that Chanda discloses that the service provider uses an Integrated Access Device (IAD) and a gateway device to provide clients with numerous service features (Ans. 15). The Examiner finds that the gateway device disclosed in Chanda corresponds to the Internet Protocol (IP) services aggregation switch (Ans. 15). The Examiner finds that the IAD disclosed in Chanda corresponds to the Enhanced Integrated Access Device (EIAD) (Ans. 15).

Further, citing MPEP 2111.04, the Examiner finds that the limitation "'to provide a bidirectional QoS ... 'is merely an intended result of the above limitations therefore; it is not given weight" (Ans. 15). Yet, to provide support for the claim limitations, the Examiner finds that Chanda discloses a class of policy which corresponds to the QoS between the clients and the service provider (Ans. 15, FF 2). In addition, the Examiner finds that Chanda discloses a traffic shaper that is used to control the traffic in both directions (bidirectional) inward and outward between the client and the service provider according to the class of policy (Ans. 15, FF 3). Therefore, the Examiner concludes that Chanda meets the claim limitation of "VPN manager adapting at least one of said IP services aggregation switches and at least one of said ElAD to provide a bidirectional QoS for at least one IP flow" (Ans. 15).

Claims 1 and 18 recite “said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS (quality of service) for at least one IP flow." Claims 2, 4-17 depend from claim 1. Claims 19-20 depend from claim 18.

Claim 25 recites "providing configuration parameters to at least one of said IP services aggregation switches and at least one of said EIADs in response to said user request and said profile associated with said user request, said at least one of said IP services aggregation switches and at least one of said EIADs adapted by said configuration parameter to satisfy said parameter of said VPN, said parameter of said VPN comprising a bidirectional QoS for at least one IP flow." Claims 33-36 depend from claim 25.

Claim 35 recites "providing configuration parameters to at least one of said IP services aggregation switches and at least one of said EIADs in response to said user request or said profile associated with said user request, said at least one of said IP services aggregation switches and at least one of said EIADs adapted by said configuration parameter to satisfy said parameter of said VPN, said parameter of said VPN comprising a bidirectional QoS for at least one IP flow." Claim 36 depends from claim 35.

Appellants contend that the combination of Chanda, Pirot, and Duffield fails to teach or suggest the limitation of "said dynamic VPN manager adapting at least one of said IP services aggregation switches and at least one of said EIAD to provide a bidirectional QoS (quality of service) for at least one IP flow" as required by claim 1 (App. Br. 14).

Specifically, Appellants contend that Chanda merely states that IADs may be configured to provide different services to clients communicating using the IADs and Chanda discloses that the gateway devices may be configured to provide different services to clients communicating through the IADs (App. Br. 15, FF 2). Appellants contend further that although Chanda states that the network system as a whole may allow services to be provided to the clients, such as enabling clients to purchase different amounts of bandwidth according to their needs, and further, that the IADs and gateway devices may be configured to provide such services to the clients, Chanda is devoid of any teaching or suggestion of adapting both an IAD and a gateway device to provide a service to the client (App. Br. 15, FF 2). Rather, Appellants contend that Chanda merely describes configuration of the IADs and the gateway device individually (App. Br. 15).

Although Chanda discloses that a customer can purchase a different amount of bandwidth according to their needs and that clients may be provided with the ability to dynamically increase or decrease the amount of bandwidth purchased in real time, we agree with Appellants' argument that Chanda does not disclose a dynamic VPN manager that adapts both an IAD and a gateway device to provide bidirectional QoS for at least one IP flow as required by claims 1 and 18 (FF 2). Specifically, Chanda discloses that a service provider can provide certain features to its clients; yet Chanda does not disclose a VPN manager or a dynamic VPN manager that provides customer network management and policy server functions as claims 1 and 18 require (FF 2). More particularly, Chanda does not disclose a dynamic VPN manager that modifies or adapts at least one of the gateway devices (IP services aggregation switches) or IADs (EIADs) to provide bidirectional QoS for at least one IP flow as the claims require.

We do not agree with the Examiner that the foregoing limitation is an "adapted to" or an "adapted for" clause that "should not be given weight"

(Ans. 15). Claims 1 and 18 require that the dynamic VPN manager adapts or modifies at least one of the IP service aggregation switches and at least one of the IADs. We agree with Appellants that this claim element is not found in either of the cited references.

We find, however, that the combination of Chanda, Pirot, and Duffield does disclose the claim limitations of claims 25 and 35. In particular, each reference enables the customer to configure certain service parameters based upon customer request (FF 2, 4, and 7). Chanda discloses that the gateway devices may be configured to provide different services to clients communicating through the IADs (FF 2). Chanda, further, discloses that each client may purchase a different amount of bandwidth according to his or her needs; wherein each client is provided with the ability to dynamically increase or decrease the amount of bandwidth purchased in real time (FF 2). Pirot discloses a system and method of controlling and managing, wherein a VPN customer may use a customer network management unit 170 to perform dedicated network management functions or may run a remote service management subsystem user interface hosted on a small portable computer to access a network database (FF 4 and 5). Duffield discloses the customer may manage the interface between the customer networks and the associated hoses in a hose VPN system, wherein the service level agreement (SLA) may be based upon one or more QoS requirements (FF 7).

Therefore, we find that the combination of Chanda, Pirot, and Duffield does not teach all the limitations of parent claims 1 and 18. Thus, we find error in the Examiner's rejection of claims 1, 2, and 4-20 under 35

U.S.C. § 103(a) as being unpatentable over Chanda in view of Pirot and further in view of Duffield, and we will not sustain the rejection.

We, however, find that Appellants have not shown error in the rejection of parent claims 25 and 35. Thus, we do not find error in the Examiner's rejection of claims 25-30 and 33-36.

Claims 21-24 and 31-32

Appellants argue that claim 21 is patentable over the cited prior art because the claim depends from claim 18 and because Forslow does not cure the deficiencies asserted with respect to the combination of Chanda, Pirot, and Duffield (App. Br. 22).

As noted *supra*, we reversed the rejection of claims 18 and 25 from which claims 21-24 and 31-32, respectively, depend. We have reviewed Forslow (the additional reference applied by the Examiner to reject these claims), and find that this cited reference does not teach the limitations deemed to be absent from the combination of Chanda, Pirot, and Duffield.

We therefore reverse the Examiner's rejections of claims 21-24 and 31-32 under 35 U.S.C. § 103, for the same reasons expressed with respect to the § 103 rejection of parent claims 18 and 25, *supra*.

CONCLUSIONS OF LAW

Appellants have shown that the Examiner erred in finding that the combination of Chanda, Pirot, and Duffield teaches a dynamic VPN manager that adapts at least one of the IP services aggregation switches and at least one of the EIAD to provide a bidirectional QoS (quality of service) for at least one IP flow within a system that dynamically manages an IP Virtual Private Network (VPN).

ORDER

The Examiner's rejection of claims 25-30 and 33-36 is affirmed. The Examiner's rejection of claims 1, 2, 4-24, 31, and 32 is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

ELD

WALL & TONG, LLP/
ALCATEL-LUCENT USA INC.
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702